# Legal Sector Affinity Group (LSAG) – Advisory Notes

These notes are supplementary to the main LSAG guidance and do not supersede them.

It is not for your supervisor to provide specific legal advice and/or confirmation on the application of the money laundering regulations (MLRs). You are required to satisfy yourself on your legal/regulatory obligations under the MLRs and that you have complied with them.

While care has been taken to ensure that these Advisory Notes are accurate, up to date and useful, members of the LSAG will not accept any legal liability in relation to this Advisory Note (which has not been HM Treasury approved).

## Note 1. Remote Working, Client Interaction and associated use of AML technology

Legal practices and practitioners should be aware that criminals will look to take advantage of people who work or meet/interact with clients remotely.

Legal Sector Anti- Money Laundering (AML)/ Counter-Terrorist Financing (CTF) supervisors understand and support the desire of practices and practitioners to vary how they work, recognising that innovation and change are fundamental aspects of strong AML control. This includes the different ways of undertaking customer due diligence (CDD), appropriate levels of identification and verification (ID&V) particularly where clients cannot be met face-to-face.

In line with a risk-based approach, the MLRs provide flexibility in the application of their requirements. There exist options for practices seeking to comply, while also working remotely.

Please note legal practices and practitioners in scope of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) (the MLRs) must still comply with their statutory requirements at all times.

### Identification and Verification

When it is not possible or desirable to undertake ID&V in person, using suitable identification documents, you should consider what risks this may create.

An inability to conduct in person ID&V does not mean you cannot complete CDD, but you may need to consider using other methods that give you the necessary assurance that the person is who they say they are.

Practices and practitioners are reminded to adopt a risk-based approach, taking into account the contents of their practice-wide risk assessment, policies and procedures (and where necessary updating them) and the circumstances of and risks presented by individual clients/matters (please see LSAG Guidance Part 1 section 5 for further information).

As an alternative to face-to-face documentary verification, legal practices and practitioners may adopt or further utilise electronic means of ID&V where appropriate to the risks present in the client/transaction.

Such methods may include (but are not limited to):

1. Digital ID&V services that meet the requirements of the MLRs R28(19) - "secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity.")
2. Gathering and analysing additional data to triangulate the evidence provided by the client, such as geolocation, IP addresses etc.
3. Verifying phone numbers, e-mails and/or physical addresses by sending codes to the client's address to validate access to accounts.
4. Using live and/or recorded digital video (many reliable and free options exist for this) of the customer showing their face and original photo identification documents so that you can compare them to a scanned copy of the same document (e.g. passport or driving licence).

No matter what ID&V service or procedure is used, the responsibility to make sure the ID&V is undertaken correctly, is with the relevant practitioner and practice. If you are placing reliance on others to conduct CDD under Regulation 39, e.g. an instructing solicitor or accountant, you should ensure that you understand how they have adapted their CDD procedures to the different circumstances.

Make sure that you keep a record and evidence of the processes you follow; for example, a set method for how video calls are to be conducted and recorded as well as a log of any video calls you make.

These methods alone may not be sufficient where the money laundering and terrorist financing risks inherent in the particular client or matter are greater. In high risk situations, further verification (including verification of source of funds/wealth) will likely be required.

Where you need to update ID&V records for existing clients, you should not rely on old ID just because you cannot currently meet them face-to-face. This is not an acceptable approach because it is unlikely to address the risk present in the transaction.

Further, information and advice may be available on your supervisor's website. You are also referred to section 7 of the LSAG Anti-Money Laundering Guidance for the Legal Sector (2021).

**Digital Identification and Verification Services**

If you are considering whether to use a digital ID&V service, you must carefully consider whether it provides the assurance needed. In order to make this judgement, you may have regard to the Financial Action Task Force (FATF) guidance on Digital Identity, particularly recommendations 22-27 in the Executive Summary as summarised below.

1. Understand what the service actually does i.e. what checks is it doing and what databases is it checking, if any and how often are any checks refreshed to ensure they are drawing on the most up to date information.
2. Take a risk-based approach to relying on the service including understanding the assurance level provided and that it is appropriate to the risk.
3. Understand whether the service provides levels of assurance and how these may be appropriately used in different circumstances.
4. Consider whether using the service, negates the idea that all non- face to face transactions are high risk.
5. Use anti-fraud, sanctions compliance and other cyber security processes to support the service.
6. Engage with the service provider to ensure the practice has access to the information it may need to prove its compliance to its supervisor or to law enforcement.

Another important consideration is whether the service has attained any accreditation or certification from any of the bodies listed in Appendix D of the FATF guidance.

**Other issues to consider when working remotely**

You should consider whether your policies, controls and procedures remain appropriate and whether they need adjustment to reflect the ways and methods by which your practice is conducting business. For example, if CDD or EDD processes change then an update of the practice-wide risk assessment, any client/matter risk assessment, and other relevant policies, procedures or controls may be necessary.

Further (non-exhaustive) examples include:

- If staff are working away from the office, ensuring they have access to the necessary CDD documentation to be able to fully consider the risks of any client or matter.
- Record keeping processes may need to be adapted to ensure compliance with regulatory requirements.
- If using digital video or photography to support CDD, or obtaining other personal information, you should obtain consent from the data subject for the capture and storage of this information and have due regard to data protection requirements.
- If you are requesting that personal or sensitive information be sent by email or other electronic means in support of CDD, due consideration should be made to the associated

information security risks. You should consider and record the necessary steps to mitigate such risks (e.g. encryption).

- Requisite ongoing AML training may be deliverable remotely or via digital means (e.g. via webinar, or video-conferencing facilities) and you should consider what adaptations your practice must make to ensure compliance where staff are working remotely.

If you have questions about whether a specific ID&V method is allowable or any other aspect of the above, contact your supervisor. If necessary, obtain independent legal advice from an experienced legal practitioner.

## Note 2. Impacts of economic instability

Economic instability can change the risks faced by legal practices and practitioners. It also has the potential to reduce economic viability or income streams – which may in some cases increase risk appetite, increase money laundering risk or lead to a reduction of requisite controls

(Non-exhaustive) examples include:

- De-prioritisation of compliance work including
    - placing more competing burdens on individuals with compliance responsibilities either due to a lack of resource (e.g. other staff to fulfil compliance responsibilities) or due to existing staff having to split their time with more emphasis on fee-earning duties
    - less financial capacity to use technology and other compliance support services (e.g. external training providers)
- Seeking to alleviate financial pressure by accepting greater levels of risk from clients and matters onboarded in order to seek increased income
- Accepting sources of capital into the business to ensure financial viability, without undertaking requisite checks on the source of this funding.
- Undertaking or transacting in areas of legal practice they are unfamiliar with, and in which consequently, AML risks are less well understood or mitigated by existing policies, controls and procedures.

When the economy enters a period of uncertainty, practitioners and practices should be particularly alert to the following red flags in new or prospective clients

- Being asked to work with unusual types of client or on unusual types of matter
- Resistance from a client regarding compliance with due diligence checks, for example being pressured to forego necessary due diligence checks or to “speed up” the process

- Becoming involved in work that is outside of the practice's or practitioner's normal area of experience/expertise – without full understanding of the money laundering and counter terrorism risks associated with the new area of work
- Any attempt to gain access to your client account where not accompanied by the provision of legal services
- Transactions where the business rationale for the transaction is not clear.

Always ensure that you are comfortable as to your understanding of the matter, including its purpose and why it is happening in the particular way it is happening. Recording risk assessments, documenting due diligence undertaken is crucial at all times.